AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions and listings of claims in the application:

1. (Currently Amended) A method of secure PIN processing in a network transaction between a terminal and a merchant server, wherein the merchant server establishes a network connection between the terminal and a transaction manager, such that the merchant server is not privy to data exchanged between the terminal and the transaction manager, the transaction manager performing the method comprising the steps of:

generating terminal data and HSM data;

sending the terminal data to ~~a~~ the terminal, wherein the terminal generates corollary data relating to a PIN using the terminal data and user input data;

receiving the corollary data ~~generated from user input and terminal data~~ from said terminal;

sending the corollary data and the HSM data to a hardware security module, wherein the hardware security module calculates the PIN based on the corollary data and the HSM data, and wherein the hardware security module encrypts the PIN and generates a PIN block that includes the encrypted PIN; and

receiving ~~a~~ the PIN block ~~generated from corollary data and HSM data~~ from said hardware security module, generating a transaction request including said PIN block and transmitting said transaction request to a financial network for authentication of the PIN and the transaction.

2. (Currently Amended) The method of claim 1, wherein said terminal data includes at least one ~~algorithms~~ algorithm.

3. (Previously Presented) The method of claim 1, wherein said terminal data includes seed data.

4. (Currently Amended) The method of claim 1, wherein said user input data includes cursor location data.

5. (Currently Amended) The method of claim 1, further comprising the step of receiving transaction data from the terminal and including said transaction data in said transaction request.

6. (Currently Amended) The method of claim ~~5~~ 1, further comprising the step of ~~generating a transaction message using said PIN block and said transaction data~~ if the financial network authenticates the PIN and the transaction, receiving a transaction approval message from the financial network and notifying the merchant server that the transaction has been approved.

7. (Currently Amended) The method of claim ~~6~~ 1, further comprising the step of ~~sending said transaction message to a financial network~~ if the financial network does not authenticate the PIN or the transaction, receiving a transaction denial message from the financial network and notifying the merchant server that the transaction has been denied.

8. (Cancelled)

9 (Cancelled)

10. (Currently Amended). The method of claim ~~9~~ 1, wherein said encrypted PIN is encrypted using a split-knowledge key.

[*Remainder of page intentionally blank*]

11. (Currently Amended) A system for secure PIN processing comprising:

a transaction manager for managing a transaction between a terminal and a merchant server, wherein the transaction manager generates terminal data and HSM data;

a transaction module executed by the terminal and communicably connected to said transaction manager for receiving the terminal data from the transaction module, generating corollary data relating to a PIN using the terminal data and user input data, and sending the corollary data to the transaction manager, wherein the merchant server is not privy to data exchanged between the terminal and the transaction manager;

a hardware security module communicably connected to said transaction manager for receiving the corollary data and the HSM data from the transaction manager, calculating the PIN based on the corollary data and the HSM data, encrypting the PIN and generating a PIN block that includes the encrypted PIN; and

wherein said transaction manager ~~sends terminal data to said transaction module such that the transaction module generates corollary data using said terminal data and user input data and said transaction manager sends said corollary data and HSM data to said hardware security module, such that the hardware security module generates a PIN block using said corollary data and said HSM data~~ receives the PIN block from said hardware security module, generates a transaction request including said PIN block and transmits said transaction request to a financial network for authentication of the PIN and the transaction.

12. (Previously Presented) The system of claim 11, wherein said transaction manager is communicably connected to said transaction module by an open network.

13. (Previously Presented) The system of claim 11, wherein said transaction manager is communicably connected to said hardware security module by a direct connection.

14. (Previously Presented) The system of claim 11 wherein said user input data comprises cursor location data.

15. (Previously Presented) The system of claim 11 wherein said terminal data includes an algorithm.

16. (Previously Presented) The system of claim 11 wherein said HSM data includes an algorithm.

17. (Currently Amended) The system of claim 11, ~~further comprising a financial network,~~ wherein ~~said transaction manager sends a transaction message including said PIN block to said financial network~~ if the financial network authenticates the PIN and the transaction, the transaction manager receives a transaction approval message from the financial network and notifies the merchant server that the transaction has been approved.

18. (Currently Amended) The system of claim ~~17~~ 11, wherein ~~said financial network sends an authorization to said transaction manager in response to said transaction message~~ if the financial network does not authenticates the PIN or the transaction, the transaction manager receives a transaction denial message from the financial network and notifies the merchant server that the transaction has been denied.

19. (Cancelled)

20. (Cancelled)

[*Remainder of page intentionally blank*]